ISS-P-005

IC 内部の回路構成変更が秘密鍵の取得性に与える影響の評価

郡　義弘† 藤本　大介† 林　優一† 崎山　一男†† 三浦　典之††† 永田　真†††
† 奈良先端科学技術大学院大学　　††電気通信大学　　†††神戸大学

1. はじめに

レーザーを用いた故障注入攻撃 [1]への対策手法として、回路内部の電圧変動をモニタリングすることでレーザーの照射を検知し、暗号モジュールへの電源供給を遮断する回路レベルの対策手法が提案されている[2]。一方、こうした回路構成の変更を行う対策技術を搭載した場合、IC 内部の電気特性が変化し、機器から漏えいするサイドチャネル情報に差異が生ずることで、パッシブ攻撃への耐性が低下する能性がある。そこで本稿では、対策回路を搭載した IC から生ずるサイドチャネル情報を電磁波として計測・解析し、回路構成変更がパッシブ攻撃への耐性に与える影響評価を行う。

2. 電源遮断回路の構成

評価対象となるレーザー攻撃への対策である電源遮断回路動の概略を図 1 に示す。対策回路では、演算を行うコアの電源供給路に MOS スイッチを追加しており、レーザーの照射検知によるフラグ遷移によって電源供給路の遮断およびコア電源のグラウンド間の短絡によるコアの停止を行う。

3. 実験条件構成

本実験では、対策回路を搭載した IC のパッシブ攻撃への耐性を評価するために、対策回路を搭載した IC と非搭載の IC における、機密情報の取得性の比較を行う。具体的には、搭載コアと非搭載コアを切り替え可能な AES を搭載した IC を使用し、FPGA を用いて IC を制御する。実験では任意の平文を FPGA から送信し、AES 実行時に生ずる波形を磁界プローブにより取得した。また、本実験では、AES の 10 ラウンド目を対象として相関電力解析（CPA: Correlation Power Analysis）を用い、秘密鍵情報の抽出を行った。

3.1. 実験結果

実験結果を図 2 に示す。縦軸が取得に失敗した部分鍵の数、横軸が波形数を表している。電源遮断回路を搭載した AES コアは非搭載のコアよりも少ない波形数で全部分鍵の取得に成功していることが観測された。続いて AES 処理時に IC から発生する電圧の時間領域における波形を図 3 に示す。図より電源遮断回路を搭載したコアでは波形の振幅が減少しており、タイミングも遅れていることが分かる。これらの結果より、電源遮断回路を搭載した場合、IC 内部の電気特性が変化することで、漏えいする電圧波形の時間及び周波数領域の特性に変化が生じ、その結果、SNR が変化することで、秘密鍵の取得性に差異が生じたと考えられる。

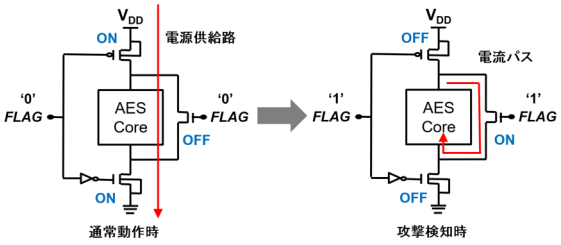

図 1:電源遮断回路の概要

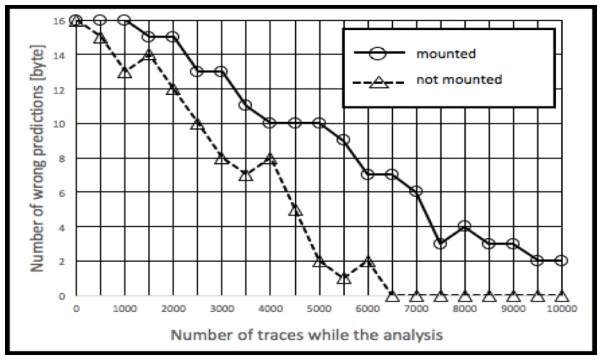

図 2: 秘密鍵取得性の比較結果

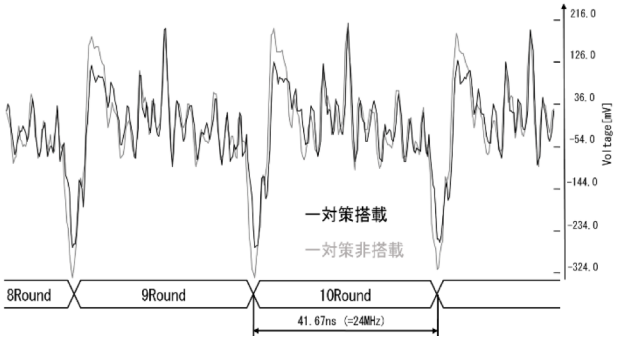

図 3:対策の有無により変化する漏えい波形の比較

4. まとめ

本研究ではレーザーを用いた故障注入攻撃への対策手法として提案されている電源遮断回路がパッシブ攻撃に与える影響の評価を行った。実験結果から、電源遮断回路を搭載した IC では回路内部の電気特性が変化し、IC 外部に漏えいするサイドチャネル情報の特性を変化させることが観測され、アクティブ攻撃である故障利用攻撃への対策回路はパッシブ攻撃への対策としても有効に働くことが確認された。

謝辞

本研究は JSPS 科研費 15H01688 の助成を受けたものです。

参考文献

[1] SP. Skorobogatov, Ross J.Anderson, “Optical fault induction attacks,” CHES 2002.
[2] K. Matsuda, et.al., “A 286F^2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack,” Dig. Tech. Papers, IEEE Intl. ISSCC, 2018.